I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Emerging Technologies, Law Enforcement Responses, and National Security

DIANA S. DOLLIVER, PH.D.*

CONTENTS

Abstract: As emerging technologies continue to shape the landscape of criminal opportunities, disruptive and destructive threats from state and non-state actors in the cyber domain challenge the ability of nations to respond to and defend their citizens and infrastructures. Cyberspace has been recognized as a distinct national security policy matter since 1998, and national security experts have since monitored the global balance of cyber power and trends in cyberattack vectors. However, the discourse surrounding

*Assistant Professor, The Department of Criminology and Criminal Justice, The University of Alabama; Academic Director, Joint Electronic Crimes Task Force, The University of Alabama. DLDolliver@ua.edu.

national security with regard to the cyber domain has not routinely and explicitly defined the role of urban and rural local law enforcement agencies or examined these institutions' ability to address a broad range of cyber threats. As such, this paper first examines an emerging technology, the Tor Network, that employs anonymizing software and facilitates attack-based, processual, and economic cyber threats. The law enforcement model in the U.S. is then explicated, detailing challenges related to fragmentation that hamper the ability of some local police departments to adequately respond to these threats. This paper concludes with proposals for strengthening the cyber capabilities and situational awareness of local police departments nationwide, emphasizing the need to consider the role of local police in future national cybersecurity strategies.

The very technologies that empower us to create and to build also empower those who would disrupt and destroy. – Pres. Barack Obama, 2009

I. INTRODUCTION

Emerging technologies continue to shape the landscape of criminal opportunities within the digital ecosystem and challenge traditional criminological understandings of victim-offender interactions. The pervasiveness of threats in the digital medium both from state and non-state actors also challenge nations' preparedness to respond to and defend against disruptive and destructive threats. Historically, the U.S. has taken an offensive stance in the cyber domain and has comparatively lacked in its defensive capabilities, leaving the country "vulnerable in this wired world," particularly due to the substantial dependence and reliance on the cyber domain for infrastructural and governmental services (DoD 2015, 1; Valeriano and Maness 2012). Further, the U.S. has been identified as the main target nation "that dissident groups, terrorist, and rogue states wish to damage" (Valeriano and Maness 2012, 145). Thus, the federal government, together with the U.S. military and intelligence communities, have identified cyberspace as a distinct national security policy area since 1998 and have subsequently developed numerous national cyber strategies, assessments of existing policies and procedures, risk assessments, and planned future actions (e.g., DoD 2005, 16; DoD 2015, 2; OMB 2018, 3; Lin 2012; White House 1998, 6).

National security experts have explicated the scope of potential cyberattacks, the development of cyber power and influence in this domain, and national cyber-based mobilization techniques, (e.g., Betz and Stevens 2011, 13; DoD 2015, 2-3; Kuehl 2009, 48; Lin 2012; Rattray 2009, 253), which explicitly require action from the federal government and implicitly require coordination with and support from local and state agencies. However, the discourse surrounding national security with regard to the cyber domain has not routinely examined how the complexity of cyber threats are handled by these latter agencies. Local police agencies have had a "silent partnership" with technology for decades, with increasing reliance and dependence on the cyber domain for investigational uses, communication purposes, case management, criminal database hosting, and data storage (e.g., Couret 1999, 1-3; Sanders, Weston, and Schott 2015, 713). Yet, as crimes in the digital arena are divorced from traditional notions of "place," law enforcement agencies have had to work within the decentralized model of policing to adapt to the changing digital environment. These agencies face many challenges however, including: fragmentation, lack of resources and training, and aging technologies.

This paper examines the complexity of the cyber domain in the current digital age with regard to the numerous and varied threats in cyberspace that are related to, and in many cases, originate from emerging technologies, and the challenges faced by law enforcement agencies in adapting to this new reality (e.g., Bossler and Holt 2012, 167; Goodman 1997, 478; Wall 2007, 3). Particular attention is paid to local police departments, as fragmentation and other issues highlight the differential impact of law enforcement responses to cyber threats. This study takes the following course: first, this discussion focuses on emerging technologies that employ anonymizing software that facilitates attack-based, processual, and economic cyber threats. Next, the law enforcement model in the U.S. is explicated, detailing inherent challenges within the decentralized policing institution that impact cyber-related responses to these threats. This paper concludes with proposals for strengthening the cyber capabilities and situational awareness for local police departments nationwide. Without a strong cyber foundation at the local policing level for both urban and rural departments, national cybersecurity strategies implemented by the federal government will be inherently weakened and the U.S. will continue to trail its rivals in defensive capabilities.

II. CYBER THREATS ON AN ANONYMOUS PLATFORM: THE TOR NETWORK

Emerging technologies are making it increasingly harder for law enforcement agencies to keep pace, as new file systems, operating systems, cloud computing capabilities, storage mediums, and Internet of Things (IoT) continue to relentlessly evolve. Within the realm of emerging technologies are those that have been developed to enhance the user's level of privacy in cyberspace. Internet platforms that utilize anonymizing software (i.e., software that obfuscates the user's location and browsing activities) are known colloquially as the "darknet." The Tor Network is arguably the most widely used network featuring darknet software, though other such networks exist (e.g., i2P, FreeNet). Given its widespread use, this discussion will focus specifically on Tor.

The Tor Project is a 503(c) nonprofit organization located in Cambridge, Massachusetts. The concept for Tor was developed in the 1990s; researchers sought to create a network that would enable secure communications between individuals located anywhere in the world. The U.S. government (e.g., the U.S. Naval Research Laboratory, National Science Foundation) and other private organizations (e.g., Google) began funding this effort in the mid-2000s (TorProject 2018a), and in the late 2000s Tor was released to the public, which introduced noise into the network. That is, if a private network was restricted to a limited number of individuals (e.g., government officials) and external intruders breached the network, these intruders would know that every user is high value target. Releasing the network "into the wild" ensures enhanced anonymity for users, as potential attackers would not be able to discern one user from the next.

The Tor Network utilizes darknet technology to obfuscate network traffic via a series of relay nodes, which ensures Tor users' IP addresses and browsing habits remain anonymous while on the network. Further, Tor-specific sites use the "*.onion*" domain, though clearnet sites (i.e., the open Internet) are also accessible from the Tor browser. As the browser is free to download from torproject.org, the Tor Project promotes this network to family and friends ("people like you and your family use Tor to protect themselves, their children, and their dignity while using the Internet"), businesses ("to research competition"), and activists ("whistleblowers use Tor to safely report on corruption") (TorProject 2018b). At the time of this writing, there are approximately 2.5 million daily users on Tor (Tor Metrics 2018) and despite the legitimate benefits of the network, these added layers

of security and anonymity have attracted more than the Tor Project's target user-base; criminal activities on Tor, particularly with regards to drug trafficking, have been well documented by researchers (e.g., Christin 2012, 7-9; Dolliver and Kuhns 2016, 322; Dolliver and Love 2015, 79-84; Soska and Christin 2015, 41-42).

A plethora of marketplaces currently exist on Tor that function similarly to Ebay and Amazon. Administrators operate large, international Tor sites that host vendors from around the world who set up virtual "shops" within the sites that offer an abundance of both legal and illegal goods and services for sale. Such items include drugs, stolen personal data, e-guides, malware, and hackers-for-hire (Dolliver and Love 2015, 80-81). Popular such marketplaces operating at the time of this writing include Dream Market, Wall Street Market, Valhalla, and Point Market. As these major marketplaces often ban the sale of weapons, child pornography, and murder-for-hire (for instance), vendor-specific websites (i.e., sites hosted by one vendor) exist to fulfill this demand. Additional sites on Tor host forums and personal websites that contain underground hacking groups and terrorist-related materials. To further conceal the existence of these sites, Tor is not an indexed network – there is no search engine analogous to Google Chrome to comb through the tens of thousands of sites on Tor as one would use on the clearnet, though some individuals have attempted to create smaller "homemade" search functions on Tor (e.g., Grams, Fresh Onions). Moreover, "*.onion*" URLs are non-identifiable; they are often a random combination of numbers and letters, so it is generally not possible to discern the content of the site from the URL alone. These additional anonymizing features present challenges not only for law enforcement investigations, but also for Tor users seeking to access these sites.

This discussion serves to highlight the complexity and extensive range of threats within the cyber domain related to the emerging technologies specific to the Tor Network. There is no limit to what cyber adversaries can target, and these threats can be loosely categorized as cyber offensive (or attack-based) threats, cyber-processual threats, and economic threats. These categories are by no means mutually exclusive or exhaustive but serve to provide a useful discussion framework.

A. *Cyber Offensive Threats*

Cyber offensive (or attack-based) threats are those designed to disrupt or inflict (virtual or kinetic) damage to a specific target, which

may be a particular server or network, or an individual or groups of people. These types of attacks include "plug and play" malware code, such as ransomware, mobile phone exploits, remote access trojans (RATs), DDoS attacks, and viruses, which are readily available for purchase on popular Tor marketplaces (Figure 1).[1] These tools can be used to breach networks, shut down websites, and extort individuals or corporations. Additionally, little technical expertise is needed; vendors often offer their services to customize the malware to fit the customer's needs, or simply sell "ready to go" malware code that any customer need simply to deploy. Though these attacks may cause minor disturbances or data loss when targeting the average person, these types of offensive attacks may lead to a significant breach of national security should efforts be focused on high priority targets, such as under-secured networks for critical infrastructures (e.g., power grids, voting machines) or mobile devices used by government officials. Further, these various forms of malware are relatively easy to purchase and deliver electronically via Tor with little risk of the transaction being detected or intercepted by law enforcement.

[1] For security purposes, the specific website names and URLs for the Tor sites discussed in this paper are withheld. If you are a researcher or law enforcement official and would like to request further information on these sites, please email justification to the author.

Figure 1. Available Malware for Purchase on Tor Marketplaces[2]

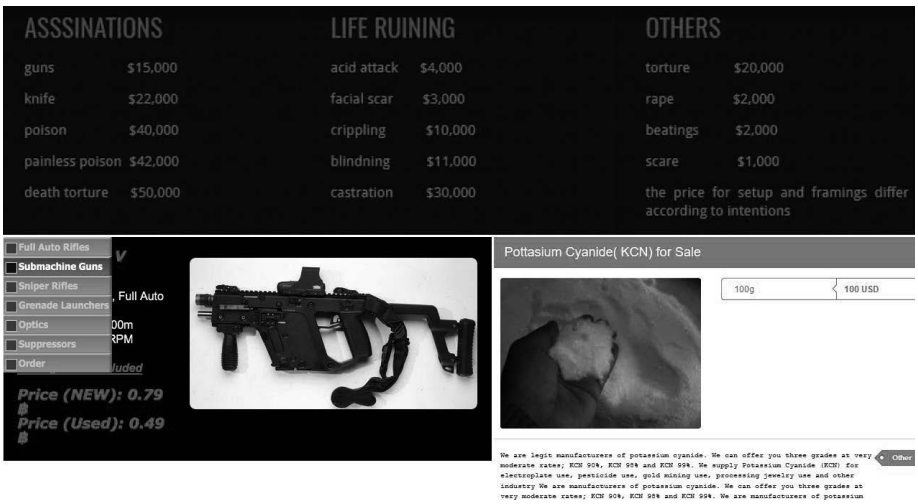
Huge Bot Pack (Google, Facebook, Youtube, Twitter) And More!	[redacted](1552) Level 5 Trusted	From **$2.99**/Piece
Very strong VIRUS - steal data and control any PC	[redacted](50) Level 1	From **$1.90**/Piece
DDos ELITE - Destroy Apache Server in 5 minutes!	[redacted](24) Level 1	From **$6.99**/Piece
Bitcoin stealing virus 2018 - get unlimited BTC !	[redacted](50) Level 1	From **$3.99**/Piece
The Complete Hacking Course: Go from Beginner to Advanced	[redacted](1) Level 1 Trusted	From **$10.10**/Piece
GhostSquad DDOS + Botnet Tools	[redacted](1552) Level 5 Trusted	From **$2.99**/Piece
Spytech Spyagent Keylogger	[redacted](210) Level 3	From **$2.99**/Piece

Attack-based threats on Tor also include kinetic components, such as murder-for-hire sites, which often offer other violent services (e.g., beatings, poisoning, or otherwise harming the target individual; school bombing services), and sites that sell weapons and weapons-related items (e.g., machine guns, grenade launchers, ricin, RPGs, potassium cyanide, handguns, ammunition, silencers, C4, bomb-making manuals, large-scale attack planning guides) (Figure 2). These items and services are not generally found on common marketplaces, with the exception of some poisons. Many major marketplaces on Tor hesitate to allow vendors to advertise such weapons and chemicals for fear of drawing the attention of law enforcement agencies; thus, sites

[2] Vendor names are redacted.

that offer these items are harder to locate and access than others. Moreover, as weapons and chemicals are tangible items, vendors take additional steps to ensure the contents of their shipments are not easily detectable by postal services (Dolliver and Kuhns 2016, 322). The potential for significant damage inflicted on an individual or large group of people via these items and services is self-evident.

Figure 2. Kinetic Threats and Services Available on Tor Sites



B. *Cyber-processual Threats*

Cyber-processual threats are those that enable or facilitate additional criminal activity, such as counterfeit documents (e.g., passports, fiat currency,[3] identification), the use of particular cryptocurrencies, hacking, and encrypted communications. Members of criminal or terrorist organizations (for instance) who seek to travel under different aliases can readily locate counterfeit passports, driver's licenses, and ID services (Figure 3), in addition to counterfeit fiat currencies from a myriad of countries, on a majority of international Tor sites and individual vendor shops. Also, fairly abundant are hacking services; hackers may offer their assistance on their own Tor site or advertise their products on common marketplaces. These products include selling WiFi hacking tools,

[3] "Fiat currency" refers to legal tender whose value is supported by the sovereign government that issued it (e.g., U.S. dollar, British pound, Polish złoty).

breaching networks to steal intellectual property or plant child pornography, and hacking into social media accounts.

Figure 3. Counterfeit U.S. Driver's Licenses and ID Services on Tor Marketplaces[4]

The use of cryptocurrencies (i.e., virtual currencies) and encrypted communications are certainly not unique to Tor or other platforms that utilize darknet software; indeed, the use of Bitcoin is becoming increasingly common among the general public as more companies and retailers around the world are accepting purchases with this currency. There are many more cryptocurrencies than just Bitcoin, however; at the time of this writing, there are currently 1,624 different cryptocurrencies in existence (CoinMarketCap 2018). Moreover, the majority of Tor sites – both large marketplaces and individual vendor shops – accept payments *only* in certain cryptocurrencies, though this was not always the case. Bitcoin relies on a public-private key cryptography to store and spend money, and cryptographic validation of transactions (Böhme, Christin, Edelman, and Moore 2015, 216). No centralized authority regulates Bitcoin or other cryptocurrency trades, and, therefore, the value of these currencies often fluctuates substantially. Each 'spent' Bitcoin is logged as a transaction (via blockchain technology) and all dealings are recorded via a public transaction history (Blockchain 2018); this public ledger identifies the wallet address(es) of the originating and receiving parties, the transaction amount, and the date and time of the transaction. Since

[4] Vendor name is redacted.

there is no regulatory oversight of this virtual currency, the user does not need to provide accurate personal information in order to buy or complete transactions with Bitcoin; however, the ability for anyone to publicly identify and monitor wallets and exact transaction amounts has led to the development of other forms of cryptocurrencies designed with superior levels of anonymity, such as Monero. Monero utilizes anonymizing technologies (e.g., ring signatures[5] and confidential transactions) to obfuscate the origins, destinations, and transaction amounts by (among other methods) splitting each transaction into multiple, smaller transactions of varying quantities – these smaller, random amounts are recorded onto the public blockchain.[6] The implementation of ring confidential transactions (ringCT) in mid-2017 has made it increasingly difficult for anyone to trace the total transaction amount or the wallets and users involved (Moser et al. 2018, 149). These features are highly attractive to those buying and selling illegal goods and services on Tor, which is evidenced by the increasing number of Tor sites accepting Monero and other harder-to-trace cryptocurrencies as forms of payment.

Further, the Tor Network supports multiple means of encrypted communications, which adds additional layers of security and privacy for users beyond the Tor browser's basic darknet features. For instance, Tor hosts encrypted messaging services (e.g., Briar, Ricochet, Tor Messenger, TorChat, SecureDrop) that work in conjunction with mainstream instant messaging protocols (e.g., Facebook, Twitter, Jabber). Additionally, Tor hosts a number of secure darknet email providers, including ProtonMail, Mail2Tor, Torbox, Lelantos, and AnonInBox. Messages sent via these services and others specific to Tor marketplaces are often further encrypted with PGP (i.e., "pretty good privacy"). While these services protect sensitive, non-criminal communications, these services also facilitate the planning, intelligence sharing, and coordination of criminal enterprises. As these levels of encryption cannot be broken, these services ensure that even if law enforcement officers intercepted

---

[5] "Ring signatures" refers to a practice by which multiple entities (i.e., the actual signer/individual and prior transaction outputs) are required to digitally approve or otherwise authorize a transaction before it can occur. This helps mask the origin of a transaction.

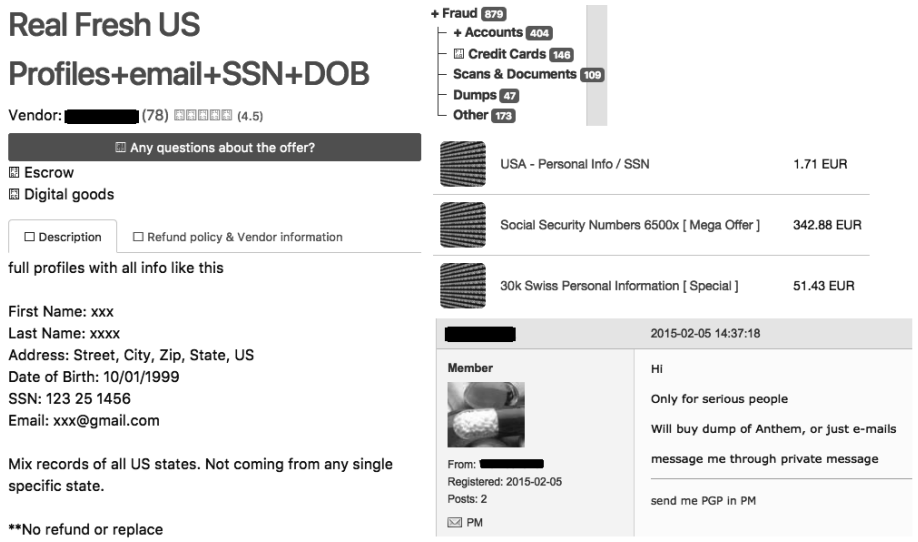
[6] For more information on Monero and fungibility, see https://getmonero.org (last accessed February 28, 2019) [https://perma.cc/8H56-NCKX].

messages or emails, the content of the communications could not be discerned.

C. *Cyber-based Economic Threats*

Cyber-based economic threats are those that financially impact individuals, private sector companies, and government institutions, such as data breaches involving stolen personal or corporate data, corporate espionage, and banking information. Batches of stolen personal data are readily available on many major Tor sites, though often individuals will host their own carding sites (i.e., sites that traffic stolen credit cards, bank account information, and personal data) on Tor. This information is often very cheap, with stolen identities (i.e., full names, SSNs, date of birth, and addresses) generally selling for roughly $1 or less each. On February 4th, 2015, Anthem disclosed that hackers had breached its network and exposed an estimated 79 million medical records (Pierson 2017); one day later, interested buyers surfaced on popular Tor marketplaces seeking access to the stolen data (Figure 4).

Figure 4. Stolen Personal Data Available on Tor Sites



Taken together, these threats have the capacity to impact individuals, agencies, businesses, and nation-states from thousands of miles away, shielded by the security provided by the Tor Network. The

cyber domain in general has challenged traditional criminological notions of "space" and "time" as the global community is becoming increasingly interconnected via cyberspace (Aas 2007, 104). This has created unique criminogenic asymmetries (i.e., "structural discrepancies, mismatches, and inequalities") that have been intensified by globalization processes (Appadurai 1996; Passas 1999, 402). That is, offenders no longer need to be within close geographic proximity to their targets, and a single individual has the ability and potential power to inflict substantial damage to critical infrastructures, breach cyber physical systems, and threaten national security (Dolliver and Love 2015, 75).

III. THE U.S. LAW ENFORCEMENT MODEL, THE SIGNIFICANCE OF LOCAL POLICE, AND FRAGMENTATION

As previously stated, the federal government (including the intelligence and military communities) conducts a range of activities "to improve collective cybersecurity and protect U.S. interests" from foreign and domestic adversaries operating in the cyber domain (DoD 2015, 3). These activities include building alliances and partnerships abroad, strengthening relations with the private sector, and enhancing information sharing and interagency coordination (DoD 2015). The last point is of particular interest and is one that has been often reiterated in national security strategies during Presidential administrations dating to the late 1990s, but yet has not been fully explicated beyond mentioning the roles of federal entities (e.g., Department of Homeland Security, Department of Defense, Office of the Director of National Intelligence, Federal Bureau of Investigation, National Security Agency) (e.g., *Cybersecurity Information Sharing Act 2015*). Information sharing and interagency cooperation related to cyber threats in the United States requires the assistance and participation of local and state agencies, though little attention has been paid to the cyber readiness and capability of these entities to investigate and defend against all types of cyber attacks and other crimes facilitated by the cyber domain and emerging technologies like Tor.

Perhaps the lack of consideration of these agencies is due in part to the decentralization of the policing institution in the U.S., whereby separate sovereign jurisdictions and legal frameworks define federal, state, and local law enforcement roles and legal authority. In this decentralized system, federal agents serve as investigators; these agents do not routinely patrol communities, respond to calls for

service (CFS; i.e., 911 calls) or interact with the public in the same way that local, municipal police officers do. As such, federal investigations often involve strategic intelligence collecting and case building that may take years, whereas local police officers utilize intelligence for tactical (i.e., more immediate) purposes. This traditional model of law enforcement in the U.S. is effective in defining the scope and foci of investigations, as each agency is responsible for addressing crimes that impact their unique jurisdiction and that are within their legal authority (e.g., local police departments do not investigate violations of federal law that occur within their municipality, such as bank robberies, and federal agencies are given particular jurisdictional authority as defined by each specific agency's mission and statutory authorities).

Significant cyber threats have historically been discussed in relation to nation-state responses, which inherently involve federal intelligence and law enforcement agencies. However, as societies become increasingly interconnected around the world, the cyber domain presents additional opportunities for asymmetric threats to impact local communities, in which local agencies serve as first responders. More closely examining the local policing structure in the U.S. and the challenges related to the cyber-adaptation of these agencies underscores the need for further attention and consideration, as threats that are not mitigated at the local level may escalate to those of national concern. Additionally, cybercrimes that impact local areas may be linked to larger, national cyber threats. This is evidenced by the number of local police departments that have been infected with ransomware, foreign state-actors breaching voting systems in both cities and small, rural towns, and state-sponsored network intrusions that compromise home and office routers (Hatmaker 2017; FBI 2018; Franescani 2016).

Historically, policing in the U.S. has been based on the "localization" of criminal events; that is, crimes have involved the convergence of the suspect(s) and victim(s) in the same geographic locale, and "space" and "time" have been closely tied to law enforcement jurisdictions. Yet, the digital age has complicated the understanding of these concepts for local police departments, confounding where "crime scenes" are located and how perpetrators victimize their targets (Bossler and Holt 2012, 166-67; Burns et al. 2004, 478; McQuade 2006, 36-39; Swire 2009, 110-11; Wall 2007, 32). These factors have presented numerous challenges to the traditional policing model, as it has become less-clear which agency is responsible for investigating various incidents. For instance, if a

person's wallet was stolen from their vehicle and contained $350, the victim would report the theft to the local police and a traditional investigation would ensue. However, if the same individual's online banking credentials were stolen, resulting in a loss of $350, the local police department would be unlikely to investigate this case even though a theft had occurred in their jurisdiction. First, this individual is not likely to report the theft to their police department, which contributes to the significant "dark figure" of cybercrime (Bidgoli and Grossklags 2016, 2; Tcherni-Buezzo et al. 2016, 8). Further, if the victim did report the loss to police, an investigation of this kind requires some degree of technical proficiency and computer resources to track down the offender, who would likely be located in a different city, state, or country. Local police departments do not often have the capacity to investigate these types of criminal incidents, resulting in the theft being uninvestigated and the victim either being reimbursed by their financial institution or absorbing the financial loss themselves. Should the cyber means by which the perpetrator used to steal the banking credentials violate federal law, it remains unlikely that a federal agency would investigate the case due to the minimal loss incurred. The inability of many police departments to investigate simple online theft also highlights the lack of ability to address attack-based, processual, or economic threats facilitated by the Tor Network. As discussed below, many officers remain generally unaware of darknet technologies, encrypted communications, and cryptocurrencies.

Without greater adaptation to cyber threats by local police departments, these cases will continue without consequence for offenders and may encourage further criminogenic behavior. One particular set of challenges that complicates such adaptation involves technological fragmentation, which is an inherent element of the decentralized model of policing in the U.S. Fragmentation occurs because of the sovereign independence between agencies, and refers to the differences in operational resources and personnel of each agency at the local, state, and federal levels. This in turn differentially impacts the capacity for each department to respond to cyber (or other) threats within their jurisdictional authority. Fragmentation is most acutely evident at the local policing level; there are approximately 18,000 local police departments in the U.S. and over half of these departments have ten or fewer officers operating in rural towns across the country (BJS 2016, 1; Peak 2014, 301). This underscores the limited capacity of many police departments *ceteris paribus*. These departments operate on restricted budgets determined

by the Mayors of the cities they serve, and each department determines how funds are allocated to meet the needs of that particular department. Thus, the equipment (e.g., less-than-lethal weapons), technology (e.g., computers, servers, networks, databases), and personnel (e.g., percentage of cyber-savvy officers and analysts per department) vary between agencies.

Fragmentation allows local police departments to better serve their particular communities – officers in rural beats likely have little need (for instance) for less-than-lethal options for crowd and riot control, while officers in urban areas may find these technologies useful. However, fragmentation can also lead to communication issues between agencies, as police departments often use different radio frequencies and equipment, and limited budgets for smaller police departments often yield outdated technology and vulnerable network infrastructure. As such, fragmentation differentially impacts police departments across the U.S., as larger departments can more easily afford infrastructural upgrades, access to bigger candidate pools and thus cyber-capable recruits, and specialize their workforce to adapt to the changing environment. Consequently, larger police departments in theory have a greater capacity to respond to and investigate a wide range of cyber threats and network intrusions facilitated by emerging technologies than smaller departments, though recent studies have shown that even officers in some large cities had little experience handling or responding to basic cybercrime complaints (Bossler and Holt 2012, 167; Swire 2009, 116).

One significant limitation of technological fragmentation for many law enforcement agencies is the capacity to process digital forensic evidence seized during active criminal investigations. In the digital age, both traditional crimes and cyber-specific threats involve at least one device containing digital evidence (e.g., mobile phones, servers, laptops, routers, CCTV footage). For instance, at the Joint Electronic Crimes Task Force (JECTF; a digital forensic laboratory operated by a local law enforcement agency in Alabama), the average number of devices per case was roughly 3, while one case in 2016 contained 38 separate devices that required significant amounts of time to process (Dolliver, Collins, and Sams 2017, 129). The types of crimes these devices were seized in conjunction with included theft, child exploitation, murder, online banking fraud, aggravated assault, cyber stalking and harassment, and rape.

With only four full-time examiners, the JECTF is the largest locally operated digital forensic laboratory in the state. The task force serves over 40 local, state, and federal agencies and has a backlog of

roughly 2-3 months (128); by comparison, other digital forensic laboratories in Alabama had backlogs of approximately 18 to 24 months or more. Some federal agencies, such as the FBI, have their own in-house digital forensic capabilities, but overall, this is an extremely specialized field that has a limited presence in law enforcement agencies across the country. This is primarily due to the significant costs required to house such capabilities. For instance, one Cellebrite UFED Touch alone (i.e., hardware to process evidence from one mobile phone at a time) costs roughly $10,000 per unit, plus an additional $4,000 for each UFED software license and subsequent annual renewal (Dolliver, Collins, and Sams, 2017, 132). These are costs (in addition to training and hiring qualified personnel) that many local police departments cannot easily assume, though agencies at all levels of law enforcement are becoming increasingly overwhelmed with the need to identify and seize devices that may contain digital evidence of criminal activity, recognize virtual currency wallets and apps used for encrypted communications, and expediently process the digital evidence. As societies continue to become interconnected with and increasingly dependent on the cyber domain (e.g., IoT), the number of devices that are linked to cybercrimes and threats, such as those facilitated by the Tor Network, will continue to increase.

Moreover, significant gaps in research exist on how fragmentation has impacted the ability of law enforcement agencies in the U.S. to conduct darknet investigations. Prior studies have largely focused on local-level police perceptions and awareness of general "computer crimes," "e-commerce," or "online property crime," whereby police have largely reported a general lack of proficiency in these types of crimes and little transparency or knowledge of methods used by upper management to address them (*see generally*, Goodman 1997; Holt and Bossler 2012; Holt, Bossler, and Fitzgerald 2010; McQuade 2006; Swire 2009; Tcherni-Buezzo et al. 2016). Little-to-nothing is known about the investigational capacities of local police agencies in the U.S. to conduct Tor-based operations or defend against darknet-originating threats, and what is publicly known relates to federal indictments and news reports once an arrest or Tor site takedown has occurred. Given that existing studies have consistently reported a general lack in basic cyber-capabilities and/or low prioritizing of cybercrime cases in municipal police departments (*see generally*, Bossler and Holt 2012; Dolliver, Collins, and Sams 2017; Holt and Blevins 2011; Holt, Bossler, and Fitzgerald 2010), additional attention is critically needed to improve the ability of departments to, for

example, seize Bitcoin or Monero, investigate the origins of a particular strain of ransomware code, or track down batches of falsified documents purchased from Tor Network vendors.

IV. Strengthening Cyber Capabilities of Local Police Departments

These challenges highlight the significant complexity that embodies the intersection of local police departments with threats in the cyber domain. Not only does the decentralized structure of policing and technological fragmentation hamper some agencies' abilities to investigate breaches of local, state, and federal laws (*see generally*, Goodman 1997; McQuade 2006; Swire 2009), but these factors also limit agencies' abilities to defend their own servers and networks from intrusion. In the digital age, these threats are no longer localized (Dolliver and Love 2015, 88); foreign adversaries can easily target municipal police departments' networks and databases from thousands of miles away. Remote intruders may put case records containing evidence and the personal information of suspects and witnesses at risk of interception or manipulation, and in the case of some small police departments, may even put an entire city's network at risk, just as intrusions into the larger network could put at risk the records of individual departments. For instance, servers of the small city of Leeds, Alabama were infected with ransomware in early 2018; this subsequently shut down operations at the police and fire departments, which also used the city's server for the department's day-to-day operations and case management (Collins 2018).

From operational and policy-driven perspectives, the primary challenge is to strengthen the cyber capabilities across local police departments within the existing decentralized model; doing so will effectively strengthen national cyber defensive and offensive capabilities. The role and importance of all local police departments should not be an afterthought of national cyber security strategies, as this level of law enforcement fundamentally forms the backbone of the cyber defensive capabilities of the U.S. Adaptation by local law enforcement to changing environments is not new; many police departments have progressed (albeit disproportionately) since 9/11 to incorporate counterterrorism units, intelligence-led policing, and participation in joint local, state, and federal law enforcement efforts, such as fusion centers and the FBI's Joint Terrorism Task Force (Price 2013, 17; Waxman 2008, 9). A similar structural shift is now needed within the cyber framework.

A. *A Multifaceted Approach: Creating Conditions for Success*

A multifaceted approach is necessary to address this primary challenge. First, the development of greater national leadership and coordination among agencies at all levels is needed beyond the legislation and policies currently in place (e.g., *Cybersecurity Information Sharing Act 2015*). Researchers have pointed out the general lack of synchronization between levels of law enforcement to address other pressing national matters (e.g., terrorism), even though local agencies are "uniquely positioned to augment federal … capabilities by virtue of being present in nearly every American community" (Riley et al. 2006, 1). Similarly, effectively addressing cyber threats (particularly those facilitated by the Tor Network) will require the strengthening of local, state, and federal partnerships, perhaps necessitating the creation of a new federal law enforcement agency focused solely on the cyber domain. Per decentralization, each federal agency currently has its own unique "cyber division," which yields distinct and isolated databases, equipment, personnel, and missions. As each federal agency is self-contained, inconsistent and (at times) conflicting information is passed down to local and state agencies. These latter agencies need more effective direction and general guidelines and standards for securing networks and databases, cyber-investigative procedures and evidence preservation, and on digital forensic tools and certifications needed for personnel to investigate Tor-based threats impacting their jurisdictions (e.g., weapons transactions). A singular federal agency responsible for cyber investigations may be able to provide improved guidance and support to local agencies in these areas.

Such a federal agency may also be better poised to assist local agencies to address nation-wide problems of personnel recruitment and retention, in addition to funding cyber-related assistance programs (Price 2013, 40; Riley et al. 2006, 1). As general recruiting practices continue to yield fewer qualified applicants and the functions of police departments become increasingly specialized (e.g., Smith 2016, 4), researchers have emphasized the "compelling need" for the federal government to support these efforts (Riley et al. 2006, 1). Moreover, a centralized cyber agency may be able to provide more widely accessible funding for local agencies to support the hiring of digital forensic experts, update existing technology (e.g., computers, servers), and better position their agencies to address criminal cyber cases. While some funding of this nature currently exists via funding sources like the National Institute of Justice, these monies are not

routinely available, funds are limited, and the process is extremely competitive. More serious consideration needs to be given to improving the cyber strength of as many of the 18,000 local police departments as feasible.

Second, officers in local police departments across the U.S. need to have a general awareness of what the Tor Network is and contains (in addition to other emerging technologies that utilize darknets), and how to preserve evidence and investigate activity on these networks. There is an overall lack of familiarity with many aspects of the cyber domain among officers (e.g., Bossler and Holt 2012, 177; Burns et al. 2004, 479; McQuade 2006, 36, 37), but as the use of Tor and cryptocurrencies become more pervasive, the need for cyber-capable law enforcement officers becomes more acute. Otherwise, local investigators may fail to recognize (for instance) handwritten cryptocurrency seeds[7] in a ledger at a crime scene, or fail to keep their own identities safe during online undercover investigations. Thus, proactive trainings in this area should be more widely available. As many agencies do not have adequate funding for such trainings, agencies may need to partner with institutions of higher learning to provide the training (Koper et al. 2015, 2). For example, a research team at the JECTF (which partners with the University of Alabama) provides free, hands-on trainings on Tor and Tails OS-based investigational methods for local, state, and federal law enforcement agencies (JECTF Law Enforcement Training Schedule). Without efforts to increase officers' situational awareness of and capabilities to address attack-based, processual, and economic threats on Tor across departments nationwide, inherent institutional fragmentation can exacerbate local, state, and national vulnerabilities and can lead to slower responses or redundancy of efforts by law enforcement agencies.

Finally, the culture within the policing institution needs to more broadly accept the realities of the cyber age. The "police culture has been widely criticized as a source of resistance to change and reform," particularly with regards to technological innovations, even though the threat landscape has been shifting into the digital arena for decades (Cohen 2017, 112; Crank 2014, 3, 4; Koper et al. 2015, 250). While cultural change is difficult not only for local law enforcement agencies, but for all organizations (Cohen 2017, 112), decreasing

[7] A seed is a random series of words that allows the individual to restore access to a wallet. Without this seed, officers will not be able to seize the cryptocurrency assets.

resistance to new technologies rests in changing the perceptions of officers, which are "highly dependent on the norms and culture of an agency and how officers view their function" (Koper et al. 2015, 20). Moreover, research on the relation between police and technology has found that officers are more likely to accept and adopt a new technology "if it is easy to use and [officers] can directly see how it helps them do their job" (Koper et al. 2015, 6). This discussion relates to the second point above, as more frequent and accessible Tor-based trainings for local law enforcement officers will ideally change the perception of this emerging technology by increasing officers' familiarity and proficiency with this anonymous platform, therefore increasing the likelihood that officers find the technology operationally beneficial. Further, the National Computer Forensic Institute (NCFI)[8] is an example of a federally driven effort to increase officer literacy in and adoption of digital forensic methods. The NCFI provides free training, equipment, and software licenses to local law enforcement officers in a broad range of digital forensic techniques, spanning from mobile device evidence collection and preservation to network intrusion detection and defense (NCFI Home Page, 2018). Introducing these technologies into police departments, along with trained personnel, will begin to normalize cyber investigations and digital evidence recovery from Tor-enabled (and other) devices, thus assisting agencies with slowly adapting to the digital age. As Cohen (2017, 122) stated, "changing [police] behavior is neither easy nor impossible."

V. CONCLUSION

This discussion underscores the gap between threats facilitated by the Tor Network that have the ability to impact national security and the differential capabilities of local law enforcement agencies in the U.S. to address and defend against those threats as first responders. Though it is difficult to unilaterally overcome issues of technological fragmentation and strengthen the cyber proficiencies of a decentralized system of 18,000 local police departments, this study proposed methods by which to improve the situational awareness and capabilities of these agencies to investigate Tor-based attack-based, processual, and economic cyber threats. In turn, this will strengthen the overall cyber defensive capabilities of the U.S. and enhance

[8] The NCFI is operated by the U.S. Secret Service and is located in Hoover, Alabama.

existing and future national security strategies. Without a strong foundation in the cyber domain at the local policing level, foreign and domestic adversaries will continue to exploit local, state, and national cyber vulnerabilities with little consequence.

Aas, Katja F. *Globalization & Crime*. Thousand Oaks: Sage Publications, 2007.

Appadurai, Arjun. *Modernity at Large: Cultural Dimensions of Globalization*. Minneapolis: University of Minnesota Press, 1996.

Betz, David and Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyberpower*. Oxfordshire: Routledge, 2011.

Bidgoli, Morvareed and Jens Grossklags. "End User Cybercrime Reporting: What we Know and what we can do to Improve it." *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, Vancouver, BC (June 2016): 1-6.

Blockchain. 2018. "Latest Blocks." https://perma.cc/DP3Z-3KGJ.

Böhme, Rainer, Nicolas Christin, Benjamin Edelmen, and Tyler Moore. "Bitcoin: Economics, Technology, and Governance." *Journal of Economic Perspectives* 29, no. 2 (Spring 2015): 213-238. https://www.jstor.org/stable/24292130.

Bossler, Adam and Thomas Holt. "Patrol Officers' Perceived Role in Responding to Cybercrime." *Policing: An International Journal of Police Strategies and Management* 35, no. 1 (2012): 165-181.

Broadhurst, Roderic. Developments in the global law enforcement of cybercrime. *Policing: An International Journal of Police Strategies and Management*. 29, no. 3 (2006): 408-433.

Bureau of Justice Statistics (BJS). "National Sources of Law Enforcement Employment Data." NCJ 249681. Last modified October 4, 2016. https://www.bjs.gov/content/pub/pdf/nsleed.pdf. https://perma.cc/9C9L-USA4.

Burns, Ronald , Keith Whitworth, and Carol Thompson. "Assessing Law Enforcement Preparedness to Address Internet Fraud." *Journal of Criminal Justice* 32, no. 2 (2004): 477-93.

Choo, Kim-Kwang Raymond. The cyber threat landscape: challenges and future research directions. *Computers and Security* 30 (2011): 719-731.

Christin, Nicolas. "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace." *Proceedings of the 22nd International Conference on World Wide Web* (2012): 213–224. https://perma.cc/9HAR-8JZD

CoinMarketCap. "Top 100 Cryptocurrencies by Market Capitalization." Accessed May 26, 2018. https://perma.cc/AG4S-RWME.

Collins, Alan. "City of Leeds Falls Victim to Ransomware Attack." WBRC. Last modified August 15, 2018. http://www.wbrc.com/story/37635768/city-of-leeds-falls-victim-to-ransomware-attack. https://perma.cc/V4GT-DJ89.

Cohen, Ryan. "The Force and the Resistance: Why Changing the Police Force Is Neither Inevitable, Nor Impossible." *University of Pennsylvania Journal of Law and Social Change* 20, no. 2, (2017): 1-19.

Couret, Christina. "Police and technology: the silent partnership." *American City and County* 99, no. 114 (1999): 31-51.

Crank, John P. *Understanding Police Culture*. New York: Routledge, 2014.

Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114-113, 129 Stat. 2242 (2015).

Denning, Dorothy. "Framework and Principles for Active Cyber Defense." *Computers and Security* 40 (2014): 108-113.

Department of Defense (DoD). "The DoD Cyber Strategy." U.S. Department of Defense. Accessed May 26, 2018. https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf. https://perma.cc/TTE5-DH3T.

Department of Defense (DoD). "The National Defense Strategy of the United States of America." . Accessed May 30, 2018. http://www.au.af.mil/au/awc/awcgate/nds/nds2005.pdf. https://perma.cc/XJ6W-DS9R.

Dolliver, Diana S., Carson Collins, and Beau Sams. "Hybrid Approaches to Digital Forensic Investigations: A Comparative Analysis in an Institutional Context." *Digital Investigation: The International Journal of Digital Forensics & Incident Response* 23, no. 4 (2017): 124-137.

Dolliver, Diana S. and Joseph B. Kuhns. "The Presence of New Psychoactive Substances in a Tor Network Marketplace Environment." *Journal of Psychoactive Drugs*. 48, no. 5 (2016): 321-329.

Dolliver, Diana and Katherine Love. "Criminogenic Asymmetries in Cyberspace: A Comparative Analysis of Two Online Marketplaces." *Journal of Globalization Studies* 5, no. 2 (2015): 75-96. https://perma.cc/QC7K-8KMK.

Franescani, Chris. "Ransomware Hackers Blackmail US Police Departments." NBC News. Last modified April 26, 2016. https://www.nbcnews.com/news/us-news/ransomware-hackers-blackmail-u-s-police-departments-n561746. https://perma.cc/FTW2-6CTJ.

Federal Bureau of Investigation (FBI). "PSA: Foreign Cyber Actors Target Home and Office Routers Networked Devices Worldwide." Alert number I-052518-PSA. May 25, 2018. https://www.ic3.gov/media/2018/180525.aspx. https://perma.cc/J5A3-FFZP.

Finklea, Kristin and Catherine Theohary. (2015). Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement. Congressional Research Service Report 7-5700: R42547.

Goodman, M.D. "Why the police don't care about computer crime." *Harvard Journal of Law and Technology* 10 (1997): 465-494.

Hatmaker, Taylor. "Russia Targeted Election Systems in 21 States, Successfully Hacking Some." TechCrunch. September 22, 2017.

https://techcrunch.com/2017/09/22/electronic-voting-state-hacking-russian-government-cyber-actors/. https://perma.cc/J93P-9XZ3.

Holt, Thomas J. and Adam M. Bossler. "Predictors of Patrol Officer Interest in Cybercrime Training and Investigation in Selected US Police Departments." *Cyberpsychology, Behavior, and Social Networking* 15, no. 9 (2012): 464-72.

Holt, Thomas J. and Kristie R. Blevins. "Examining Job Stress and Satisfaction Among Digital Forensic Examiners." *Journal of Contemporary Criminal Justice* 27, no. 2 (2011): 230-250.

Holt, Thomas J., Adam M. Bossler, and Sarah Fitzgerald. "Examining State and Local Law Enforcement Perceptions of Computer Crime." In *Crime On-line: Correlates, Causes, and Context*, 221-46. Raleigh: Carolina Academic, 2010.

Joint Electronic Crimes Task Force (JECTF). "Law Enforcement Training Schedule." The University of Alabama. Last accessed November 21, 2018. https://cybercrime.as.ua.edu/resources/jectf/training-schedule/. https://perma.cc/K9ZL-PY8J.

Koper, Christopher, Cynthia Lum, James Willis, Daniel Woods, and Julie Hibdon. 2015. "Realizing the Potential of Technology in Policing: A Multisite Study of the Social, Organizational, and Behavioral Aspects of Implementing Policing Technologies." George Mason and Police Executive Research Forum. http://cebcp.org/wpcontent/technology/ImpactTechnologyFinalReport.pdf. https://perma.cc/AP4U-T4P7.

Kuehl, Daniel. "From cyberspace to cyberpower: defining the problem." *Cyberpower and National Security*. Dulles: Potomac Books, Inc., 2009.

Lin, Herbert. "Operational Considerations in Cyber Attack and Cyber Exploitation." *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*." Washington, D.C.: Georgetown University Press, 2012.

McQuade, Sam. "Technology-Enabled Crime, Policing, and Security." *Journal of Technology Studies* 32 (2006): 32-42.

Morris, David. "Russian Hackers Targeted Election Systems in 39 States." Fortune Magazine, June 14th, 2017.

Moser, Malte, Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Shashvat Srivastava, Kyle Hogan, et al. "An Empirical Analysis of Traceability of the Monero Blockchain." *Proceedings on Privacy Enhancing Technologies* 2018, no. 3 (2018): 143-163. https://perma.cc/22PY-TKYW.

National Computer Forensic Institute (NCFI). "Home page." Accessed November 21, 2018. https://www.ncfi.usss.gov/ncfi/. https://perma.cc/QLF2-NQ4Y.

Obama, Barack. Remarks by the president on securing our nation's cyber infrastructure. Last accessed May 22, 2018. https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure2009.

Office of Management and Budget. *Federal Cybersecurity Risk Determination Report and Action Plan*. 2018. https://www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf. https://perma.cc/HMX9-FWLQ.

Passas, Nikos. "Globalization, Criminogenic Asymmetries and Economic Crime." *European Journal of Law Reform* 1, no. 4 (1999): 399–423.

Peak, Kenneth. *Policing America: Challenges and Best Practices (8th Edition)*. New Jersey: Pearson, 2014.

Pierson, Brendan. "Anthem to pay record $115 mln to settle U.S. lawsuits over data breach." Reuters U.S. Legal News. Last modified June 23, 2017. https://perma.cc/9WK6-Z9RT.

Price, Michael. "National Security and Local Police." Brennan Center for Justice Publication. Last accessed May 30, 2018. https://www.brennancenter.org/sites/default/files/publications/

NationalSecurity_LocalPolice_web.pdf. https://perma.cc/ZCV4-Z6WK.

Rattray, Gregory. "An environmental approach to understanding cyberpower." IN *Cyberpower and National Security*. Edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Dulles: Potomac Books, Inc., 2009.

Riley, K.J., Jeremy Wilson, Gregory Treverton, and Barbara Raymond. "Think Locally, Act Nationally: Police Efforts in Fighting Terrorism Need Greater Federal Leadership." RAND Periodical Review. Accessed May 30, 2018. https://www.rand.org/pubs/periodicals/rand-review/issues/spring2006/police.html. https://perma.cc/MU7L-EF28.

Robinson, Michael, Kevin Jones, and Helge Janicke. Cyber warfare: issues and challenges. *Computers and Security* 49 (2015): 70-94.

Sanders, Carrie, Crystal Weston, and Nicole Schott. "Police innovations, 'secret squirrels' and accountability: empirically studying intelligence-led policing in Canada," *The British Journal of Criminology*. 55, no. 44 (2015): 711-729.

Smith, Sid. "A Crisis Facing Law Enforcement: Recruiting in the 21st Century." The Police Chief. June, 2016. http://www.policechiefmagazine.org/a-crisis-facing-law-enforcement-recruiting-in-the-21st-century/. https://perma.cc/MR6W-KWVN.

Soska, Kyle and Nicholas Christin. "Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem." *Proceedings of the 24th USENIX Security Symposium*, August 2015: 33-48. https://perma.cc/3SAS-U4C3.

Swire, P. "No Cop on the Beat: Under-Enforcement in E-Commerce and Cybercrime." *Journal of Telecommunications and High Technology Law* 7 (2009): 107-26.

Tcherni-Buezzo, Maria, Andrew Davis, Giza Lopes, and Alan Lizotte. "The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave?" *Justice Quarterly* 33, no. 5 (2016): 890-911.

Tor Project. Tor: Sponsors. Available via https://www.torproject.org/about/sponsors.html.en (last accessed May 22, 2018) https://perma.cc/8BPR-3B2S.

Tor Project. Tor Main Page. Available via https://www.torproject.org/ (last accessed May 26, 2018) https://perma.cc/8BPR-3B2S.

Tor Project. Users. Available via https://metrics.torproject.org/userstats-relay-country.html (last accessed May 22, 2018) https://perma.cc/NHV5-DGKL.

Valeriano, Brandon and Maness, Ryan. 2012. "The Fog of Cyberwar." The Council on Foreign Relations, November 21, 2012. https://perma.cc/3CJJ-MKJF.

Wall, David. *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press, 2007.

Waxman, Matthew. "Police and National Security: American Local Law Enforcement and Counter-Terrorism After 9/11." Columbia Public Law & Legal Theory Working Papers. Accessed May 30, 2018. http://lsr.nellco.org/cgi/viewcontent.cgi?article=1049&context=columbia_pllt. https://perma.cc/UG5S-G9QD.

White House. "A National Security Strategy for a New Century." 1998. http://nssarchive.us/NSSR/1998.pdf. https://perma.cc/58AM-95ZA.